

AFRL-IF-RS-TR-2002-146
Final Technical Report
June 2002



FORENSIC INFORMATION WARFARE REQUIREMENTS STUDY

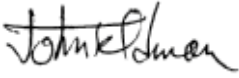
WetStone Technologies, Incorporated


APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

**AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2002-146 has been reviewed and is approved for publication.

APPROVED: 
JOHN FELDMAN
Project Engineer

FOR THE DIRECTOR: 
WARREN H. DEBANY, Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> <i>OMB No. 074-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE JUNE 2002	3. REPORT TYPE AND DATES COVERED Final Jun 98 – Feb 99	
4. TITLE AND SUBTITLE FORENSIC INFORMATION WARFARE REQUIREMENTS STUDY			5. FUNDING NUMBERS C - F30602-98-C-0243 PE - 62702F PR - 4600 TA - AI WU - PI	
6. AUTHOR(S) C. Hosmer and G. Gordon				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) WetStone Technologies, Incorporated McNeil Building 17 Main Street, Suite 237 Cortland New York 13045			8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/IFGB 525 Brooks Road Rome New York 13441-4505			10. SPONSORING / MONITORING AGENCY REPORT NUMBER AFRL-IF-RS-TR-2002-146	
11. SUPPLEMENTARY NOTES AFRL Project Engineer: John Feldman/IFGB/(315) 330-2664/ John.Feldman@rl.af.mil				
12a. DISTRIBUTION / AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.				12b. DISTRIBUTION CODE
13. ABSTRACT (Maximum 200 Words) The study presents an analysis of the state of the art in computer forensic technologies employed by the military, law enforcement, and business and industry sectors. Additionally, it charts the observed deficiencies in this area, by providing a research and development roadmap of consolidated requirements of all sectors of the economy which rely on the existence of a robust forensic toolset for accomplishing forensic computer investigations. An extensive survey of existing forensic tools was performed in order to develop a Forensic Information Warfare (FIW) Matrix that provides an in-depth look into the issues and the state-of-the-art technologies being used. The Computer Forensics matrix permitted the development and refinement of a FIW research and technology Road Map that integrates data from the FIW Matrix, with on-going university research, industry interests, and real forensic case data needs. The results provide a solid framework for determining the requirements for future R&D thrusts in computer forensic science.				
14. SUBJECT TERMS Computer Forensics, Forensic Tools, Computer Forensic Science, Cyberforensics, Network Forensics			15. NUMBER OF PAGES 36	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

Table of Contents

1	DOCUMENT SUMMARY	1
2	FORENSIC INVESTIGATION TECHNOLOGIES	1
2.1	TERMS USED	2
2.1.1	Key Words.....	2
2.1.2	Bit Stream Image.....	2
2.1.3	File Slack	2
2.1.4	Peripheral Based Data.....	3
2.1.5	Windows Swap File.....	3
2.1.6	Temporary Files.....	3
2.1.7	Unallocated Space	3
2.1.8	Boot Record Data.....	4
2.2	FORENSIC EXAMINATION STANDARDS	4
2.2.1	Key Computer Service Guidelines.....	4
2.2.2	IACIS.....	5
2.2.3	JMac Enterprises	7
2.3	INTERVIEWS WITH USERS	7
2.4	PROVIDERS OF FORENSIC INFORMATION SERVICES	8
2.4.1	Judd Robbins, Computer Expert Witness.....	8
2.4.2	Computer Forensics Inc.	8
2.5	TOOLS & TECHNOLOGIES USED	8
2.5.1	Expert Witness.....	9
2.5.2	Ontract Data Advisor.....	10
2.5.3	SafeBack.....	11
2.5.4	ViewDisk	11
2.5.5	AdaDisk LE.....	11
2.5.6	IPFILTER V2.1 - (Internet Analysis Tool)	12
2.5.7	NTI-DOC Forensic Tool	12
2.5.8	CRCMD5 Data Validation Tool.....	12
2.5.9	DiskSig Bit Stream Data Validation Tool	12
2.5.10	FILELIST Disk Catalog Tool:.....	12
2.5.11	FILTER_1 Intelligent Filter (Advanced Filter).....	12
2.5.12	GETSLACK (Ambient Data Collection Tool):	13
2.5.13	TextSearch PLUS:	13
2.5.14	DIBS Portable Evidence Recovery Kit.....	13
2.5.15	Recover98.....	13
3	TECHNICAL PAPERS & PANELS	14
3.1	ADVANCING CRIME SCENE COMPUTER FORENSICS TECHNIQUES.....	14
3.2	USING SMARTCARDS AND DIGITAL SIGNATURES TO PRESERVE ELECTRONIC EVIDENCE	15
3.3	TIME-LINING COMPUTER EVIDENCE	16
3.4	COMPUTER FORENSICS: GATHERING EVIDENCE FOR CORPORATE AND LAW ENFORCEMENT PURPOSES	16
4	MEETINGS & CONTACTS	17
4.1	ECII BOARD OF DIRECTORS MEETING	17
4.2	GLOBAL INTEGRITY / SAIC MEETING	19
4.3	COMPUTER FORENSIC INTEGRATED PRODUCT TEAM (IPT) MEETING	19
5	AGENCY RESEARCH	19
5.1	NEW YORK STATE POLICE FORENSIC INVESTIGATION CENTER	19

5.1.1	<i>Observations of FIC Capabilities</i>	19
5.1.2	<i>Areas of Difficulty</i>	22
5.2	FEDERAL BUREAU OF INVESTIGATION	23
5.2.1	<i>FBI - CART</i>	23
6	FORENSIC CASE INVESTIGATION BY WETSTONE	25
7	SYRACUSE UNIVERSITY LEGAL STUDY	25
8	COMPUTER FORENSICS RESEARCH & DEVELOPMENT CENTER	25
8.1	TRACES TECHNICAL JOURNAL	25
8.2	CFRDC WORKSHOP - COMPUTER FORENSIC SYMPOSIUM	26
9	FUTURE RESEARCH	26
9.1	FIW TECHNOLOGY MATRIX	26
9.2	COMPUTER FORENSICS TECHNOLOGY ROADMAP	26
9.2.1	<i>Background</i>	27
9.2.2	<i>Interviews Conducted</i>	28
9.2.3	<i>Key Findings</i>	28
10	REFERENCES	31

Figures and Tables

FIGURE 9.1	COMPUTER FORENSICS MATRIX	26
FIGURE 9.2	TYPICAL INTRUSION DETECTION SYSTEM DEPLOYMENT	27
FIGURE 9.3	COMPUTER FORENSICS TECHNOLOGY ROADMAP “THE GAPS”	29
FIGURE 9.4	COMPUTER FORENSICS TECHNOLOGY ROADMAP “FUTURE THREATS”	30
FIGURE 9.5	COMPUTER FORENSICS TECHNOLOGY ROADMAP “CORE TECHNOLOGIES”	30
TABLE 5.1	ANALYZING COMPUTER EVIDENCE	21

1 Document Summary

The purpose of the effort was to analyze the current state and sophistication of the computer forensic strategies, and the available products and technologies, Government-of-the-shelf (GOTS) and contractor-of-the-Shelf (COTS), used to examine information assets for evidence. This knowledge can help establish a framework for future research in the area and establishing computer forensics needs for all sectors of the economy. Forensic tools can be used *after* an information attack, to identify the intruder his motivation, and perhaps predict the next attack phase. To obtain a complete cross section of the current state-of-the-art in computer forensics, this study includes forensic technologies employed by the military, civilian law enforcement, as well as by business & industry.

We investigated the information assurance paradigm being used by the DoD today, and have conducted an extensive survey in order to develop a Forensic Information Warfare (FIW) Matrix that provides an in-depth look into the issues and the state-of-the-art technologies being used by the military, law enforcement, and business/industry. With the enhanced understanding of Computer Forensics derived from the matrix creation, we developed a FIW Technology Road Map that integrates collected data from the FIW Matrix, in-process university research, industry participation, and actual forensic case data. The FIW Matrix and the resulting FIW Technology Road Map provide a solid framework from which to determine the requirements for the next step in enhancing the detect/react portions of the DoD information assurance paradigm.

Finally, we conceptualized and built the Computer Forensic Research & Development Center (CFRDC). This consortium of business, industry, government, education and law enforcement was established to advance the state-of-the-art in FIW.

2 Forensic Investigation Technologies

Our findings indicate that most tools being used to collect data off a computer disk drive do nothing more than copy the drive and search the data found there (including files, slack area, and unallocated space) along with information that may be found on peripherals and back up media. A search is then conducted (either manually or with pattern matching tools) for numbers, words, or phrases that may be used as computer evidence. We have therefore divided the processes of Forensic Computing into three main areas:

1. Image Capture - The imaging process is fundamental to any computer investigation. The process of imaging should not alter any information on the target machine. The normal procedure of taking the image to WORM media allows the investigator to search for evidence without jeopardizing the integrity of the original data.

2. Image Processing - The processing software consists of processes that index and extract text from all areas of the target image. Options are also available to perform a full extraction of files from the image if required.
3. Investigation - Once the processing has taken place, full searches of all areas of the disk takes only seconds. Multiple searches for any combination of characters can be made. Frequently used words may also be set up as a library under a 'group' name for enhanced searching. Postcodes or phone numbers can be identified easily.

2.1 Terms Used

2.1.1 Key Words

In order to fully understand the processes and methodologies employed by those organizations providing services and products in the area of computer forensics and electronic evidence retrieval, it is necessary to describe a few of the terms used in computer forensics.

When analyzing retrieved information, computer forensic specialists look for key words and phrases within the stream of data obtained during a search. They are trying to find out if the computer was being used to store important information such as dates, phone numbers, names of contacts, etc., in order to piece together materials and provide evidence to support strategies. These key words in most cases are the words of the street, for example drug “street talk”, arsonist vocabulary, child pornography words and phrases, or other criminal lingo. In addition to key words that they use to find evidence, they also must search for words that would cause them to not examine a document or file due to it containing information that would be privileged. For example, in the search of a person’s house for paper documents that may be incriminating, detectives use care to ensure they don’t examine documents that are communications between the suspect and their wife, attorney or priest. The same care must be taken when examining electronic documents.

2.1.2 Bit Stream Image

A Bit Stream Image of a computer’s storage systems provides a physical copy of the data. This copy does not rely on the logical contents of the drives in question, but copies the information bit-by-bit onto another device where the searches and analysis is performed.

2.1.3 File Slack

File slack is a data storage area of which most computer users are unaware. It is a source of significant ‘security leakage’ and consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. Specialized forensic tools are required to view and evaluate file slack and it can prove to provide a wealth of information and investigative leads. Like the Windows swap file, this source of ambient data can help provide relevant key words and leads that may have previously been unknown.

On a well used hard disk drive, as much as 900 million bytes of storage space may be occupied by file slack. File slack should be evaluated for relevant key words to supplement the keywords found by other means.

2.1.4 Peripheral Based Data

Many laser printers retain in memory the last few pages to be printed. If the memory is electronic and the printer is left powered on, then this information may be accessible. Even if the laser printer is turned off, it may store this information on hard disk, and the information will remain during the power off. Since printers often have the storage capacity to store an entire document, most computers actually create a “print file”, commonly known as a spooler file, which is then sent to the printer piece by piece. These spooler files can continue to exist, even after the document in question is printed. Hard cards (circuit boards that act as disk drives) can also contain valuable data that should not be overlooked. Finally, electronic devices such as modems, pagers, and especially fax machines, contain significant amounts of memory that can be accessed and saved.

2.1.5 Windows Swap File

The Windows swap file is a potentially valuable source of evidence and leads. The Windows swap file acts as a huge data buffer, and many times fragments of data or even an entire word processing document may end up in this file. As a result, careful analysis of the swap file can result in the discovery of valuable evidence when Windows is involved. This tedious task was done in the past with hex editors and the process took days to evaluate just one Windows swap file. By using automated tools, that process now takes just a few minutes. When Windows 95/98 is involved, the swap file may be set to be dynamically created as the computer is operated. This is the default setting and when the computer is turned off, the swap file is erased. However, not all is lost because the content of the swap file can easily be captured and evaluated by current applications. These programs automatically capture erased file space and create a file that can be evaluated by other programs.

2.1.6 Temporary Files

Word processing programs and database programs create temporary files as a by product of the normal operation of the software. Most computer users are unaware of the creation of these files because they are usually erased by the program at the end of the work session. However, the data contained within these erased files can prove to be most valuable from an evidence standpoint. This is particularly true when the source file has been encrypted or the word processing document was printed but never saved to disk. Like magic, these files can be recovered.

2.1.7 Unallocated Space

The DOS and Windows ‘delete’ function does not completely erase file names or file content. Many computer users are unaware the storage space associated with such files merely becomes unallocated and available to be overwritten with new files. Pointers to the data are all that is changed, the data is not actually erased from the drive. Unallocated space is a source of significant ‘security leakage’ and it potentially contains erased files

and file slack associated with the erased files. Often the DOS Undelete program can be used to restore the previously erased files. Like the Windows swap file and file slack, this source of ambient data can help provide relevant key words and leads that may have previously been unknown to the computer investigator.

2.1.8 Boot Record Data

The Boot Record from a computer contains information relating to the programs that were *loaded* when the computer was started or *booted*. If this information has been compromised an attacker can load any program and have it run at startup.

2.2 Forensic Examination Standards

We have researched a number of agencies and organizations that provide guidelines and services related to computer forensics and the extraction of data from seized computers. The following sections highlight some of our findings.

2.2.1 Key Computer Service Guidelines

A complete, competent forensic computer and data examination:

- ◆ Ensures that all examinations use properly prepared and verified forensically sterile media. This ensures that there is no contamination by viruses', by previously examined data from another or the same case, or by other data that could be on the media.
- ◆ Examines, describes, and properly documents the hardware that is the subject of the examination.
- ◆ Ensures that the original media and data are maintained in their original unaltered state during the examination. This will prevent loss of data and will be used to authenticate the validity of the data recovered. It will also be a sound defense to lawsuits claiming alteration or corruption of the data or operating system.
- ◆ Ensures that no unauthorized writes are made to the media by viruses, by "booby trap" defense schemes, by the operating system, by applications that write back to the media to cache data, or by other inadvertent means.
- ◆ Recovers, unlocks, and accesses deleted files, hidden files or data, password protected files and encrypted files. Any means of concealing the data is documented for possible use as evidence later.
- ◆ Lists all of the files in the directory hierarchy, including recovered files. The name, size, starting cluster, time and date of creation or last modification of each file is documented.
- ◆ Examines data in unallocated space (space that is not currently in use by files but which may contain data) for relevancy to the investigation or inquiry at hand. Potentially relevant data is recovered, printed, and the location where found is documented.

- ◆ Examines data in file slack (the area within the last cluster of a file that is not being occupied by the file) for relevancy to the investigation or inquiry at hand. Potentially relevant data is recovered, printed and the location where found is documented.
- ◆ Examines all normal data files individually. Relevant files are printed and the location where found is documented.
- ◆ If requested, examinations are conducted to determine the author and creation or modification date of particular documents or files, to determine who created particular directories, to determine which computer in an office or location created certain diskettes, and similar comparisons relating to document and file creation, etc.

2.2.2 IACIS

IACIS (International Association of Computer Investigative Specialists) is a non-profit corporation composed of law enforcement professionals. IACIS7 membership consists of Federal, State, Local and International law enforcement professionals including: Police, Sheriff's Deputies, State Troopers, FBI, IRS, Customs, Secret Service, DEA, INS, Postal Inspectors, Revenue Canada, RCMP, Military and other law enforcement agencies. All members have been trained in the forensic science of seizing and processing evidence from computer systems.

2.2.2.1 *Hard & Floppy Disk Examination*

The following are the IACIS7 recommended procedures for conducting a complete examination of computer Hard Disk Drive (HDD) or Floppy Disk Drive (FDD) media:

1. Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.
2. All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company.
3. The original computer is physically examined. A specific description of the hardware is made and noted. Comments are made indicating anything unusual found during the physical examination of the computer.
4. Hardware/software precautions are taken during the examination to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the examined media and other media used for the examination.
5. The contents of the CMOS, as well as the internal clock is checked and the correctness of the date and time is noted. The time and date of the internal clock is frequently very important in establishing file creation or modification dates and times.

6. A duplicate image of the original media is made. The duplicate image is used for the actual examination. A detailed description of the process and identification of the hardware, software and media is noted.
7. The copy of the original HDD is logically examined and a description of what was found is noted.
8. The boot record data, and user defined system configuration and operation command files, such as, the CONFIG.SYS file and the AUTOEXEC.BAT file are examined and findings are noted.
9. All recoverable deleted files are restored. The first character of restored files are changed from a HEX E5 to "-", or other unique character, for identification purposes.
10. A listing of all the files contained on the examined media, whether they contain potential evidence or not, is made. The listing will indicate which files were printed or otherwise recovered.
11. The unallocated space is examined for lost or hidden data.
12. The "slack" area of each file is examined for lost or hidden data.
13. The contents of each user data file in the root directory and each sub-directory (if present) are examined.
14. Password protected files are unlocked and examined.
15. A printout is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits (printouts of data) are marked, sequentially numbered and properly secured and transmitted.
16. Executable programs of specific interest should be examined. User data files that could not be accessed by other means, are examined at this time.
17. Document comments and findings.

In many instances, a complete examination of all of the data on media may not be authorized, possible, necessary, or conducted for various reasons. In these instances, the examiner should document the reason for not conducting a complete examination. Some examples of limited examinations would be:

1. The scope of examination is limited by the search warrant or the courts.
2. The equipment must be examined on premises. (This may require the examination of the original media. Extreme caution must be used during this type of examination.)

3. The media size is so vast that a complete examination is not possible.
4. The weight of the evidence already found is so overwhelming that a further search is not necessary.
5. It is just not possible to conduct a complete examination because of hardware, operating systems or other conditions beyond the examiner's control.

2.2.3 JMac Enterprises

John B. McElhatton

Voice: (703) 938-0724

<http://www.jmacent.com>

Typically, computer forensic examinations by JMac are structured as follows:

1. Preliminaries: The computer is powered off and all peripherals are disconnected. An auxiliary device to store off-loaded data is connected and the computer is booted from a clean floppy disk. The CMOS, internal hardware and software configurations, and hard disk directory structure are examined for information and leads. If passwords or other obstacles are encountered, they are either decrypted or bypassed.
2. Search: Forensic utilities are loaded into memory and directed to find specific text or patterns located within all data blocks including intact files, erased files, unallocated space, slack space, and cached areas on the hard drive(s).
3. Recovery: If pertinent data is found to reside within deleted files, they are recovered as completely as possible.
4. Retrieval: All significant data blocks are off-loaded to the auxiliary storage device for off site analysis. Data is copied in a manner consistent with established preservation of evidence protocols and with as little disruption to normal course of business as possible.
5. Analysis: Information specific to the case is extracted from all data blocks, printed out where appropriate, or converted to appropriate format for easy examination by clients or their representatives.
6. Documentation: A comprehensive and professionally bound report is prepared and presented to the client. The report details all aspects of the examination process and the results obtained.

2.3 Interviews with Users

During FIW Technology Collection, we focused on the task of obtaining information on the current technology being used by the DoD, other Government Agencies, Law Enforcement Agencies, Financial Institutions, Credit Card Companies, Insurance Firms, and IS organizations working within corporate America. We carefully examined the

current research and development underway through government and private research and development contracts.

We met with representatives of the following: The Hartford, MBNA America, First Data Resources, National Insurance Crime Bureau, and the National Fraud Center. We also participated in the Lawyer's Roundtable on Information Security where presentation were made by individuals from CERT, FBI, DoD, DOJ-Computer Crime and Intellectual Property Section, United States Secret Service, FEMA, National Security Telecommunications Advisor Council (NSTAC), President's Commission on Critical Infrastructure Protection, and the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information.

2.4 Providers of Forensic Information Services

Many agencies provide Forensic Information or Expert Witness services to individuals or agencies that have experienced computer break-ins or crimes. These service agencies are listed below with a short synopsis of their services and the products they use in their practice.

2.4.1 Judd Robbins, Computer Expert Witness

Voice: 702-832-8210
judd@knock-knock.com

Services Provided

Company has computer specialists who serve as expert witnesses and litigation consultants in intellectual property and other computer litigation cases.

Tools Used: SafeBack
Expert Witness (does not alter file dates or original media)

2.4.2 Computer Forensics Inc.

Jon Berryhill
Voice: 707-745-1405
Jberryhill@computerforensics.com

Services Provided

The company provides computer forensics services to law enforcement agencies, attorneys, private investigators and businesses.

2.5 Tools & Technologies Used

Our research has led us to a number of internal and commercial products currently being used in the forensic process. These tools and products are listed in the following sections:

2.5.1 Expert Witness

We have identified *Expert Witness*, by ASR Data Acquisition & Analysis LLC, (512)-918-9227 as a product for purchase and testing. The following information about this product was taken from the ASR web site:

Expert Witness for Windows95 is a Forensic Data Acquisition and Analysis program which has been designed based on the specifications and requirements of the law enforcement community.

Expert Witness is non-invasive to the original computer evidence. All reports and extracts are designed to provide a clear, concise chain of custody. Copies of original evidence are authenticated and verified to assure the admissibility and integrity of the copy.

Data Acquisition

Expert Witness simplifies the data acquisition process by using a "wizard" interface. The wizard walks the user through a series of simple steps and uses the responses and information provided by the user to create a case profile and acquire the evidence. The case profile contains all the information needed to establish a chain of custody for the evidence and document the data acquisition procedures.

This approach substantially reduces the amount of time spent preparing reports and the amount of training required to use the software, virtually eliminating the possibility of user errors, simple mistakes, and oversights which can jeopardize the integrity and admissibility of computer evidence.

Expert Witness provides unparalleled flexibility in the ways it can acquire evidence. The software has been developed to allow evidence to be spanned over as many destination disks as necessary. Data compression is an option which can significantly reduce the hardware requirements of storing large amounts of evidence until a case is fully adjudicated.

An entire server may be processed as evidence and stored on several inexpensive storage cartridges instead of a large, expensive hard drive which will just sit in an evidence locker.

Data Analysis

Once Expert Witness has acquired, cataloged, and authenticated the evidence, the evidence is ready to be analyzed. Expert Witness provides a powerful and intelligent search engine which uses fuzzy logic, ranked search results, and a host of features which go well beyond simply looking for text within a file.

Benchmark tests have shown Expert Witness to be several times faster than search engines offering far less, and because Expert Witness is able to search an entire case instead of a single disk at a time, only one search is required.

Expert Witness searches all the evidence on the drive. Files which meet any search criteria may be viewed instantly, even if the program which created them has been deleted.

Deleted files may be viewed, searched, and sorted before they are selectively recovered. This results in recovering relevant data quickly and easily without having to wade through hundreds, or even thousands, of deleted files which have nothing to do with the case.

Expert Witness will allow multiple users to search the same case files over a network, search multiple case files for similar information, and facilitate inter-departmental and inter- agency hand-off of case related information.

Expert Witness "learns" as it is used. Search terms, preferences, and user options can be remembered, resulting in less time spent configuring the software and more time using it.

Expert Witness can be easily configured to work with browsers, viewers, editors and other forensic software, extending it's evidence protection features to those programs as well.

The field of Computer Forensics is evolving as rapidly as the underlying technology. Expert Witness is maintained, enhanced, and updated regularly. To get the latest update, simply click on the "Update" button in the program. The software will connect to our web site and automatically download the latest version.

2.5.2 Ontrack Data Advisor

Ontrack Data International, Inc.
Minneapolis (Corporate Headquarters)
6321 Bury Drive
Eden Prairie, MN 55346
Phone: 1-612-937-5161
Fax: 1-612-937-5750
<http://www.ontrack.com>

- ◆ Self booting
- ◆ Analyzes file systems and structures
- ◆ Evaluates hard disk drive capacity, electronics and media integrity
- ◆ Checks critical boot sectors
- ◆ Reads the Master Boot Record
- ◆ Cross-checks partition tables and CMOS
- ◆ Checks system memory for defects and errors

System Requirements

- ◆ DOS versions 3.31 and greater
- ◆ Windows 3.0, 3.1 and 3.11; Windows 95; Windows 98;
- ◆ Windows NT (FAT) or OS/2 (FAT)
- ◆ 386, 486, Pentium or compatible computer
- ◆ 640K base memory, 4MB extended memory

2.5.3 SafeBack

Sydex, Inc.
P. O. Box 5700
Eugene, OR 97405
Information and Support: (541) 683-6033
FAX: (541) 683-1622
<http://www.sydex.com>

- ◆ DOS-based utility to back up and restore hard disks
- ◆ Bit stream oriented
- ◆ Accesses IDE & SCSI controlled devices
- ◆ Mirror-image backup files of hard disks
- ◆ Mirror-image copy of an entire hard disk or partition.
- ◆ Obtains master boot record and the partition tables
- ◆ Preserves all the data including inactive or “deleted” data.
- ◆ Files can be written to any writable magnetic storage device, including SCSI tape backup units.
- ◆ Cyclical redundancy checksums (CRCs) distributed throughout the backup process enforce the integrity of backup copies
- ◆ Date- and time-stamped audit trail maintains a record of operations during a session.

2.5.4 ViewDisk

Sydex, Inc.

- ◆ Finds hidden or deleted data on computer diskettes regardless of format
- ◆ Analyzes diskettes for content and consistency
- ◆ Checks for instances where a file extension may not be consistent with actual file type
- ◆ Searches any diskette by user-defined values
- ◆ Prints data on a physical sector or file basis
- ◆ Copies almost any kind of diskette without regard to format or type.
- ◆ Requires that scanned diskettes be write-protected
- ◆ Date- and time-stamped Audit Trail maintains a record of all operations during a session.

2.5.5 AdaDisk LE

Sydex, Inc.

- ◆ Searches, analyzes and copies almost any kind of diskette without regard to type or format
- ◆ Edits diskette data sector by sector
- ◆ Performs a diagnostic read of a specified diskette track
- ◆ Dumps data from a selected range of tracks into a DOS in order to examine and manipulate data from non-DOS diskettes.

2.5.6 IPFILTER V2.1 - (Internet Analysis Tool)

New Technologies, Inc.
2075 Northeast Division
Gresham, Oregon 97030 USA
503-666-6599 or (fax) 503-492-8707
<http://www.forensics-intl.com>

- ◆ Identifies patterns of Internet E-mail and browsing activity contained in Windows swap files and files created from file slack and/or unallocated file space
- ◆ Fuzzy logic based
- ◆ Output in database form

2.5.7 NTI-DOC Forensic Tool

New Technologies, Inc.

- ◆ Take an 'electronic snapshot' of files and subdirectories that have previously been identified as having some evidentiary value

2.5.8 CRCMD5 Data Validation Tool

New Technologies, Inc.

- ◆ Compares the content of one file with another (128 bit level of accuracy).
- ◆ Compares the logical content of an entire hard drive, zip drive, jazz drive or floppy diskette

2.5.9 DiskSig Bit Stream Data Validation Tool

New Technologies, Inc.

- ◆ Mathematically compares a bit stream backup with the original computer.(used with SafeBack)

2.5.10 FILELIST Disk Catalog Tool:

New Technologies, Inc.

- ◆ Catalog contents of files on separate hard disk drives or floppy diskettes
- ◆ Compatible with FAT 12, FAT 16 and FAT 32 systems
- ◆ Deals automatically with long file names

2.5.11 FILTER_I Intelligent Filter (Advanced Filter)

New Technologies, Inc.

- ◆ Relies upon pattern recognition to help in the creation of lists to be used in the search of key words on hard disk drives and floppy

- ◆ Filters binary data extracted from Windows swap files, Windows temporary files, file slack and unallocated storage space
- ◆ Aid in the identification of English words contained in binary data.
- ◆ Aid in the identification of passwords and Log-ons dumped from memory into the Windows swap file, file slack and unallocated space.

2.5.12 GETSLACK (Ambient Data Collection Tool):

New Technologies, Inc.

- ◆ Captures all file slack on a specific logical hard disk drive or floppy diskette.

2.5.13 TextSearch PLUS:

New Technologies, Inc.

- ◆ Searches hard disk drives and floppy diskettes for key words or word patterns.
- ◆ Searches Files, Slack and Erased Space
- ◆ Compatible with FAT 12, FAT 16 and FAT 32 systems.
- ◆ Can be used on Windows, Windows 95 and Windows 98 systems
- ◆ Has Both Logical and Physical Search Options
- ◆ User Defined Search Configuration Feature
- ◆ Alert for Graphic Files (secrets can be hidden in them)
- ◆ Alert for Compressed Files (text won't be found in them)

2.5.14 DIBS Portable Evidence Recovery Kit

Computer Forensic Investigations Ltd

166 Fleet Street

London EC4A 2DY

Tel: 44 (0) 171 353 3777

Fax: 44 (0) 171 353 3747

- ◆ Uses DIVA™ (Digital Image Verification and Authentication).
- ◆ Advanced cluster analysis
- ◆ Specialist undulating tools
- ◆ CD-ROM writing packages

2.5.15 Recover98

Phoenix Software Systems, Inc.

1701 Drew St. #7,

Clearwater, FL, 33755

Voice: 888-447-1291

Fax: 727-467-9145

- ◆ True 32 bit file recovery
- ◆ Windows95/98, NT4.0/5.0

- ◆ Multi-boot
- ◆ Striped, spanned & mirrored drives
- ◆ All versions of RAID
- ◆ Builds in-memory virtual file system
- ◆ Does not rely on FAT or MFT to build file system
- ◆ Allows choice of recovery method
- ◆ FAT12, 16, 32 and NTFS file systems
- ◆ SCSI, RAID, IDE and removable media

3 Technical Papers & Panels

A key aspect of the FIW program is to engage as many user communities as possible in the active discussion and advancement of forensic technologies. One important way we accomplished this was through actively publishing our findings, ideas and results. Several papers and presentations were completed during this effort and delivered to AFRL.

3.1 Advancing Crime Scene Computer Forensics Techniques

SPIE International Symposium:

Enabling Technologies for Law Enforcement & Security

Computers and network technology have become inexpensive and powerful tools that can be applied to a wide range of criminal activity. Computers have changed the world's view of evidence because computers are used more and more as tools in committing 'traditional crimes' such as embezzlements, thefts, extortion and murder. [1] In 1992, in an article entitled "Software Forensics: Can we Track Code to its Authors"[4] the authors pose the following question:

"Often we are aware of an intrusion only after it has occurred. On some occasions, we may have a fragment of code left behind – used by an adversary to gain access or damage the system. A natural question to ask is can we use this remnant of the code to positively identify the culprit?"

By expanding upon this insightful question, we believe we can more broadly define the field of Forensic Information Warfare (FIW). "Forensics Information Warfare (FIW) is the discovery, analysis, and reconstruction of evidence extracted from computer systems, computer networks, computer media and computer peripherals that allows us to answer the questions of Who, What, Where, When, Why and How." This evidence can then be used to prosecute, dismiss, or discipline the intruders, provide a road map to system reconstruction and restoration, and help us define better ways to defend our computer systems and networks. It can provide us with insight that will allow us to anticipate, and ultimately prevent an attack before it happens, or to dynamically modify our operating conditions in order to complete our objective. This new and emerging discipline of FIW is concerned with a continuum of activities [4]. These activities include 1) the collection of audit and intrusion detection data, 2) the assessment of damage to a computer resulting

from an information attack or malicious destruction of data, 3) data recovery and evidence extraction, and 4) analysis for prosecution purposes.

This paper focuses on reviewing the current state-of-the-art of the data recovery and evidence construction tools used in both the field and laboratory for prosecution purposes.

- First we report on the state-of-the-art and describe the current capabilities, strengths, weaknesses and limitations of today's technology. This includes the current state-of-the-art of Air Force technology relevant to criminal activity, espionage and examination of adversary computers seized in military operations.
- Next we discuss the changes in computer and networking technologies that are taking place now and in the near future that will adversely impact the current technologies and require additional sophistication through both automation and human interaction.
- Finally, we discuss a technology road map that we developed. This road map defines a general path for the collaboration of future research, development, user feedback, legal posturing, and commercialization of technology.

3.2 Using SmartCards and Digital Signatures to Preserve Electronic Evidence

SPIE International Symposium Enabling Technologies for Law Enforcement & Security

Digital signature technologies are being used today in many aspects of information security including proof of identity, authentication, authorization, integrity and non-repudiation.

In 1993, the COAST laboratory at Purdue University developed the concept of a software "Tripwire" [1] that would help identify if key system files have unexpectedly changed. The process was to generate a set of one-way hash values that define the contents of key system files stored on host computers. Periodically the hash's would be recalculated and compared to the stored original to determine if any change could be detected. Each unexpected result would be investigated to determine if the change was malicious or accidental and corrective action taken.

The research into this change detection is the basis of our proposed paper. We discuss how we have advanced this techniques using SmartCard and Cryptographic Tokens and how these advancements can be applied to computer evidence in the following areas:

- Application of digital signature and smart card technologies to protecting evidence at the crime scene. These techniques provide a greater level of security for the verified signatures as well as a separation of roles for signers and verifiers allowing computer evidence to carry greater weight in the court room
- Assignment of signature for the entire captured system as well as individual resources.

This allows for a separate assurance argument for distinct pieces of evidence found on the computer.

- The application of these techniques to networks of computers found at a crime scene.

3.3 Time-Lining Computer Evidence

IEEE Information Technology Conference Information Environment for the Future

In the investigation of a criminal case involving a computer or computers, the time-line of “computer events” can provide a critical piece of information relating to the prosecution of criminals, establishment of the whereabouts of certain individuals, substantiation of alibis, determination of civil liabilities, or possibly the guilt or innocence of those facing criminal charges.

Computer events or evidence such as the contents or update time of electronic documents, the time and content of e-mail communications, system logon and logoff events, the access of specific internet documents or sites, communication with known individuals in chat rooms or other collaborative means, evidence of document destruction, or the forwarding of messages to external devices such as pagers, voice mail accounts or fax machines, may provide direct clues to not only the means but also the motive of a criminal act. Extracting this information from computer systems, network infrastructures, backup media, or peripheral devices is a time consuming and tedious process, however, it can prove to be a worthwhile endeavor.

This paper describes a process to not only identify and extract this information, but to correlate it into a Time-Line with external events such as phone records, witness testimony, and physical evidence. This Time-Line can become an integral part of the road map that provides detailed information pertinent to an investigation. We also describe and define the current state-of-the-art technology that is used in this pursuit, the limitations of these technologies, and where additional research and development is necessary.

3.4 Computer Forensics: Gathering Evidence for Corporate and Law Enforcement Purposes

ECII Ninth Annual Conference Fraud Management in the Twenty-First Century

During this effort, WetStone Technologies, Inc. moderated a panel at the Economic Crime Investigation Institute’s Ninth Annual Conference (Fraud Management in the Twenty-First Century) on November 9th and 10th in Washington D.C.

This panel, entitled, “Computer Forensics: Gathering Evidence for Corporate and Law Enforcement Purposes, included the following panelists: Shiu-Kai Chin, Syracuse University, Michael Winburn, Modus Operandi, Greg Lipscomb, Litton/TASC, John Feldman, AFRL/IFGB and Gary Gordon, ECII.

Each panelist presented a short 5-10 minute talk on their area of expertise related to reconstruction of computer evidence. Open discussion with the audience occurred next. The goal was to develop a wish list for new technologies, problems commonly encountered in the field, as well as, the new challenges that continued technological advancements will bring.

4 Meetings & Contacts

4.1 ECII Board of Directors Meeting

A meeting of the ECII Board of Directors was held on September 25th. WetStone Technologies gave a briefing of our Computer Forensics program, which was well received. During the meeting, the Board's help was solicited to gather information from their respective organizations. A follow-up meeting was held the week of October 6th with the following organizations, to have a discussion with their technical people who perform Computer Forensic and fraud investigations:

- Tom Pickard, Assistant Director of the FBI
- Norman Wilox, Jr. Trans Union National Fraud Center
- Veronica Wyrwas, Global Integrity

The ECII Board of Directors is comprised of the following individuals.

Dr. Gary R. Gordon, Executive Director
Utica College of Syracuse University
Utica, New York

Mr. Tom Pickard, Assistant Director
Federal Bureau of Investigations
Criminal Investigation Division

Mr. John L. Martin, Chairman, Partner
The OSO Group Ltd.
Washington, D.C.

Mr. Gregg Bacchieri
Division President
MBNA America Bank, N.A.
Newark, Delaware

Mr. Bruce Barr
Chief Financial Officer
AT&T ISTEEL
Radditch, England

The Honorable Sherwood
Boehlert
United States Congressman
23rd Congressional District of
New York
Washington, D.C.

Dr. Matthew R. DeZee
President & Chief Executive
Officer
Tibbets Group
Hoboken, N.J.

Mr. John DiLiberto
President & Chief Executive
Officer
National Insurance Crime
Bureau
Palos Hills, Illinois

Mr. John C. Gibbons
President
The OSO Group Ltd.
San Francisco, California

Ms. Patricia Koch
Vice President of Regulatory Relations
Bell Atlantic
Washington, D.C.

Mr. Joel S. Lisker
Senior Vice President
Security and Risk Management
MasterCard International
New York, New York

Mr. Thomas McClure
Director Fraud Management
Cellular Telecommunications Industry Association
Washington, D.C.

Mr. Anthony J. Montesion
Vice President Risk Operations
AT&T Universal Card Services Corp.
Jacksonville, Florida

Ms. Ann Nestor-Hubert
Special Agent
U.S. Secret Service
Washington, D.C.

Mr. Bruce Prouty
Office Managing Partner
Arthur Andersen
Hartford, Connecticut

Mr. Robert Rasor
Director of Corporate Security
General Electric
Washington, D.C.

Mr. Gary Rudedge
EVP Issuer Risk Management
First Date Corp.
Omaha, Nebraska

Mr. Thomas W. Tarkowski
Manager, Investigations
Equitable
New York, New York

Dr. Stanley M. Welland
Group Executive
Citibank Global Technology
Infrastructure
New York, New York

Mr. George A. Williams
Chief Financial Officer
ISS Corporation
Atlanta, Georgia

Ms. Veronica Wyrwas
President, Global Integrity
McLean, VA

Mr. Norman A. Willox, Jr.
Chief Executive Officer
Trans Union National Fraud
Center
Horsham, Pennsylvania

Dr. Thomas G. Brown
Interim President
Utica College of Syracuse
University
Utica, New York

Mr. John T. Wolff
Vice President College
Relations
Utica College of Syracuse
University
Utica, New York

4.2 Global Integrity / SAIC Meeting

On October 9, we met with four individuals from Global Integrity/SAIC and SAIC. They shared in very general terms the tools and methods they use in computer forensics. They stated that their methods were proprietary, and that they could not share them without nondisclosure agreements and a clear sense of what would be in it for them.

They were very interested in the computer forensics workshop and agreed to sponsor it. Our initial observations were very similar to what we observed at the FBI. Without further discussion and disclosures, it is difficult to assess the level of sophistication.

4.3 Computer Forensic Integrated Product Team (IPT) Meeting

On August 12, 1998, WetStone Technologies, Inc., and ECII hosted the first Computer Forensic Integrated Product Team (IPT) meeting at Utica College. Presentations were given by representatives from MITRE, Litton/TASC, Johns Hopkins University, and Modus Operandi, as well as by the WetStone team. This meeting was attended by 20 professionals from the industry.

5 Agency Research

5.1 New York State Police Forensic Investigation Center

During this effort, we visited the FIC in order to gain a better understanding of their operation and their use of computer forensic technologies. The FIC is a 108,000 square foot state-of-the-art facility in Albany, NY that serves the entire law enforcement community with a full range of forensic services. The center provides forensic analyses of physical evidence collected and submitted by all facets of the criminal justice system. Current evidence submissions are divided equally between state and municipal agencies.

5.1.1 Observations of FIC Capabilities

- Forensic investigation operation is still paper based (all records, reports, etc. are kept in paper files)
- Geographic nature of the state makes communication between law enforcement agencies difficult
- The computer crimes lab is a service organization within the FIC. They never take over a case, they only provide analysis, data and expert testimony.
- Currently, New York for example, has some 156 computer laws on the books.
- Currently, the courts (defense attorneys) have challenged only certain aspects of electronic evidence. This is a positive sign that computer evidence will continue to grow in its use in the courtroom.
- Currently, parsing of authorized information extracted from computer systems is done by humans. For example, certain information is protected – such as husband/wife, doctor/patient, attorney/client and clergy/parishioner communications. No electronic solution is currently available that will assist in the separation of this information.

- Computer experts and analysts accompanying a raid, must also be named in the warrant.
- FIC uses re-writable optical disks to extract information from seized computer systems. No cryptographic technology is currently employed (such as digital signatures) to match the authenticity of the copy to the original. The copy is then used in the analysis and investigation of the seized system. The obvious limitation is that as computer systems and networked systems are used by criminals, this technique will no longer be feasible.
- Criminals are currently using a wide range of computer technology, some of which is so outdated that access to the information takes a significant amount of time. For example, the FIC continues to run into situations where they are required to extract information from computers such as the Amiga, Apple II GS, and numerous archaic versions of Unix.
- Currently most of the analysis and extraction of information is done visually by the operator with the aid of primitive computer tools. As the size and complexity of computer information is increased, the computers must be able to do the searching and analysis on behalf of the operator.
- Very limited tools are currently available for extraction of information from Unix systems and obscure operating systems.
- Access and breaking of encrypted files is virtually impossible given the tools that are currently in use. The good news is that there have only been a few incidents where encryption or steganography has been employed.
- Currently, the FIC is experimenting with tools such as Expert Witness, Safeback, Snapback, Hijack Pro, and well known tools such as Norton Utilities. The current tools appear to be developed by small companies speculating sales to law enforcement and commercial concerns. The technology employed in these tools appears not to be based in science or research, but rather appears to be tools that can only solve specific problems on known platforms within given parameters.

In order to better understand the process, tools and problems that law enforcement faces in extracting and analyzing computer evidence, we created the following table:

Table 5.1 Analyzing Computer Evidence

Stage of Investigation	Electronic Tools	Discussion
Seizing the computer	None	Currently the computer and technology are seized by the NYS Police under the rules of evidence and the warrant that they hold. The evidence is then transported to the Forensic Investigation Center (FIC) typically by the officers that collected the evidence. It is brought to the FIC and checked into the vault and secured.
Backup	Safeback, Expert Witness, Snapback	<p>The first step in the actual investigation process is to perform a bit stream backup of the device. They currently use one of the tools listed to perform the operation. There are several problems associated with the backup process. They are as follows:</p> <ol style="list-style-type: none"> 1. Backup tools won't perform the backup due to technical difficulties with the tools, age of the systems, format of the drive (doublespaced or compressed drives cause great difficulty), operating system (especially have problems with UNIX, old Macintosh devices, and new high capacity devices (9GB drive). 2. Drive compatibility with both hardware and software setups that they have in place. In some cases it may take up to two weeks to successfully create a backup. <p>Once the drive is successfully backed up they attempt to get the drive information onto read-write optical disks and create a case file in order to begin the next phase.</p>
Evidence Extraction	Expert Witness	The newest tool in the FIC arsenal is <i>Expert Witness</i> . They are working toward moving as much of the investigative process to the Expert Witness tool as possible. The tool has many advantages that allow them to deal with the raw extraction, and organization of the evidence. Searching for evidence is done currently using regular expression searches (<i>grep</i>). The investigator simply enters the searches manually. The viewing of evidence is done through built-in content viewers within Expert Witness or external views that the user adds.
Case Creation	Expert Witness	The case creation process allows the extracted information to be placed in a case file either on a floppy disk, hard disk, or removable media.
Case Analysis	None	During this process the investigators use their experience and training to search the computer evidence for documents, deleted files, images, e-mail, slack space and un-allocated disk space. They look for any information

		that will provide them with evidence.
Correlation of computer events	None	During this process the investigator attempts to piece together the different computer events in order to establish a timeline, order of events, related activities, and contradictory evidence.
Correlation with non computer events	None	During this process the investigator pieces together non-computer events (telephone records, credit card receipts, eye witness testimony, physical forensic evidence, and crime scene reports). The process here can be simple or quite difficult depending upon the case. The investigator manually attempts to sort out and correlate information.
Case Presentation	Standard Office Software	Finally, the information that has been extracted, analyzed, and correlated is put together in a form ready for presentation.

5.1.2 Areas of Difficulty

Our discussions helped us identify several limitations directly attributable to the capabilities of the available technology.

Backup of Evidence

1. Backup of evidence is slow
2. Backup of evidence is not always reliable
3. Backup of evidence requires significant technical savvy
4. Backup of large hard drives or multiple computers in many cases is not possible
5. Backup cannot always be contained to a single backup device which makes the investigation process more difficult and time consuming

Analysis of Evidence

1. Tools do a good job of extracting evidence from deleted files, slack space and unallocated spaces, and provide a good inventory of what was found.
2. Viewing of information may require them to purchase virtually every application currently used to create the data. They need a universal information viewer.
3. Searching of the data is very rudimentary and time consuming. There are no standard taxonomies of words, phrases, data formats, or data organization that could be applied to specific crimes under investigation.
4. No capability of identify possible privileged information until after they read it.
5. No technical means of identifying possible authors of the information by the vocabulary, grammar, or style used based upon other known writings.
6. No tools are available to assist in correlation of computer information from the same computer or case and no correlation between cases or evidence files is currently accomplished.
7. No tools exist to correlate other evidence with the computer evidence (including phone records, credit card receipts, eye witness testimony, Internet Service Provider (ISP) records, or other forensic evidence).

8. Capabilities to correlate the evidence from computer network breakins are limited.
9. No tools were identified that will assist them in decrypting data, breaking passwords or accessing protected information contained in electronic organizers.
10. No tools are available to develop a timeline of either computer events or non-computer events.

5.2 Federal Bureau of Investigation

On October 8, 1998 we met with key personnel at FBI Headquarters regarding data for the study. We were able to gather preliminary information on the methods, techniques, and tools used by the FBI in both Headquarters and in the field. We were invited to return to meet with the technicians and forensic specialist to see first hand the methods and tools. This meeting took place on November 10, immediately after the ECII conference.

Our initial observations were that they do not have any sophisticated tools and methods. They appear to be heavily reliant on intensive labor methods and the specific knowledge of the individuals performing the forensic analysis. They are very interested in developing better tools and root methods.

5.2.1 FBI - CART

Computer Analysis and Response Team (CART) – At this meeting, we met with the analyst and technicians in the CART laboratory. We received two demonstrations from the staff. First, we received a demo from Analysts. The ACIS tool has gone through quite a few revisions and changes over the past two years. The ACIS tool has the following basic capabilities:

1. Remote Mounting – Provides for the mounting of foreign FAT or High Performance File Systems (HPFS) found on PCs as remote devices to the NT operating system. This feature allows the tool and the analyst to work on one or many cases simultaneously. Most of these remote devices are read-write optical media that are write protected.
2. Operating System Traps – The ACIS system traps all NT – Operating disk write system calls to the remotely mounted devices and ensures that OS-Writes are not allowed to the mounted devices. This prevents any unexpected or intentional writes from occurring on the destination devices.
3. Evidence Preservation – Up until just recently the FBI used CRC protection, but since our first meeting on October 8th are now using MD5 one-way hash values to protect the contents.
4. Known File Filter – ACIS contains a Known File Filter that searches the file-system for files that can be identified, (e.g., normal system files, dll's, applications, etc). The tool automatically searches for these and eliminates the matches from the potential evidence sources reducing the search space significantly depending on the specific drive.
5. File Identification – Currently contains components that identify file types based upon the contents of the file. Currently they can identify almost 100 different file types. They cannot yet automatically identify files that employ encryption or steganography, and are interested in any solutions we could offer.
6. File Viewers – ACIS contains file viewers that allow files to be displayed from within ACIS. External viewers can also be employed. This continues to be a problem as new proprietary file formats continue to advance.

7. Searching – ACIS uses key words or phrase lists from a text file to support text searching. The entire file-system can be searched based upon this source file. This is either based on the crime type (i.e., arson) along with specific data from the case. For example, names or people, organizations, places and things involved in the case.

The most significant attribute of ACIS is its ability to chain together these “black box” tools and process the case file in off-hours. What the analyst does is set up a process. The following shows an example of concatenation of several processes:

Preserve Evidence, Run Known File Filter, Run File Identification, Search all Text Files with Keywords, Thumbnail all Graphic Files for viewing.

This selection is done graphically with the output of one “black-box” acting as the input to the next. When they return the next day the case is “done” or “cooked” and ready for analysis by the investigators. They are currently working on a standard definition for the box input / output, which then could be used by outside developers to provide additional black boxes.

5.2.1.1 Areas for Improvement

1. Larger device handling (currently limited to 2.4 GB due to optical media). If a larger volume is encountered, the data must be split between multiple optical disks. Based upon even yesterdays technology (9 GB hard drives) it would typically require 5 optical disks to hold the file system data. In the near future, this will be much higher.
2. Better file identification
3. Encryption / Steganography identification
4. Universal file viewing
5. Advanced searching that builds the input file through semantic identification
6. Evidence time-lining boxes
7. Evidence preservation using digital signatures
8. Extensive Known File Filter Databases
9. Graphic image content identification

5.2.1.2 Golden Gate

We also received a demo of Golden Gate, a technology that allows for the interconnection of a wide variety of computing platforms including PC(NT, 3.1, 95 98, DOS etc.), Novell’s Netware, Linux, SUN (SUNOS, Solaris), HP9000, and even VAX/VMS. The concept is to create a heterogeneous network with a set of tools that can provide cross platform connectivity for investigations. Instead of extracting hard-drives from seized computers, they simply connect the suspect computer to the Golden Gate network and boot the device with a special boot disk. The boot disk provides network read-only access from the Golden Gate system for evidence extraction. Once the evidence has been extracted, the results are provided to the ACIS team for analysis.

The next meeting was held with the Assistant Director of the FBI. Our discussion focused on the synergy between ECIL, CFRDC, AFRL and the CART laboratory. We discussed several possible ways we could work together. He has provided a clear path for us to have a substantive interchange between the CART laboratory and the investigators.

Finally, we met with the Section Chief of the Financial Crimes Section. We discussed the possibility of sharing information between the financial crimes unit and our study. She enthusiastically supports our effort to advance technology in this area. She has agreed to work with us to provide multiple articles for the premier issue of *TRACES* and we are working with CART team members and other financial crimes units to produce abstracts for our review. We should start receiving the abstracts by mid- December from these folks. She also agreed to send investigators to the CFRDC workshop in January to ensure that Law Enforcement was well represented.

6 Forensic Case Investigation by WetStone

WetStone Technologies, Inc. had the opportunity to perform an actual computer forensic investigation for another agency during this effort. Due to the proprietary nature of the case, the specific agency and case details will not be disclosed here. However, in order to accomplish this investigation, WetStone learned and experienced the investigative process first hand, and can provide some insight into the tools, technologies and methods that are lacking and are sorely needed, in order to effectively perform computer forensic investigations.

7 Syracuse University Legal Study

This information gained through this effort was greatly increased due to our collaboration with the Syracuse University CASE Center. WetStone Technologies, Inc., Dr. Shiu-Kai Chin of the CASE Center and Ted Hagelin, the Director of the Law Technology & Management Program at Syracuse University instantiated a group of six graduate law students who worked on expanding our investigation in the area of Forensic Computing. The students focused their efforts on two specific areas. First, to research the needs of business and industry for forensic tools in their organizations, and second, to ascertain the legal impact of these tools. Their report was delivered to AFRL and provides an in-depth look into these areas.

8 Computer Forensics Research & Development Center

We have accomplished a great deal in bringing the CFRDC to existence. We have an established location at Utica College and initial participants. We plan to continue to expand this organization with future funding and additional sponsors.

8.1 *TRACES Technical Journal*

The basis and foundation for this needed publication in the area of Computer Forensics was established during this effort, although a premier issue was not created. It is our hope that we can continue to move toward publication of this journal with additional support and funding.

8.2 CFRDC Workshop - Computer Forensic Symposium

We feel that the Computer Forensic Symposium was one of the highlights of this effort. This symposium brought together practitioners and researchers for an exchange of ideas and goals. The agenda, results and presentations from this symposium were summarized in a briefing presented to AFRL.

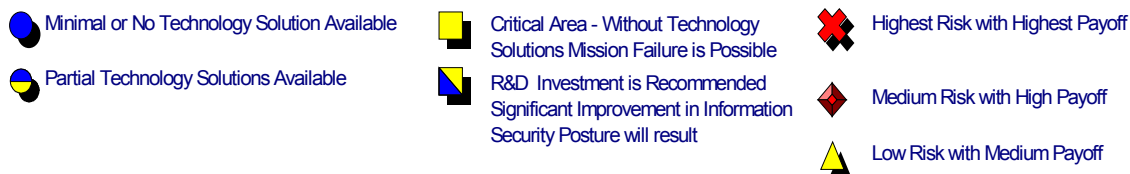
9 Future Research

9.1 FIW Technology Matrix

The FIW Technology Matrix developed during this effort, shows our representation of the relationships between Computer Forensic technology areas with the current technology state-of-the-art, current R&D and COTS focus, recommended research and the associated research risk.

Computer Forensics Matrix

<i>Technology Areas</i>	State-of-the-Art	Current R&D Focus	Current COTS Focus	Recommended Research	Research Risk
Evidence Preservation / Imaging		✓	✓		
Evidence Organization					
Evidence Extraction			✓		
Evidence Viewing		✓	✓		
Hidden Data Detection					
Hidden Data Recovery					
Evidence Timelining					
Evidence Searching			✓		
Evidence Mining			✓		
Evidence Correlation					
Network Forensics					
Case Management			✓		



1999 WetStone Technologies, Inc.

Figure 9.1 Computer Forensics Matrix

9.2 Computer Forensics Technology Roadmap

The development of the Computer Forensics Technology Roadmap required careful analysis of the collected information along with the Computer Forensics Matrix. The Roadmap identifies and recommends the steps necessary to establish a comprehensive

approach to improving the FIW technology and mitigation strategies in a dual-use fashion. The Roadmap focuses on the following areas:

1. Research and Development project areas needed to advance the state-of-the-art in the fundamental areas needed.
2. Identification of existing government, commercial and university research whose output should directly or indirectly feed into the Roadmap.
3. Identification of commercial technologies or government technologies (existing or on the drawing board) that will directly feed into the Roadmap.
4. Collection and analysis of real life data
5. Identification of current GOTS and COTS technologies where investments could be made to quickly advance FIW
6. Identification and development of enabling technologies that will allow developers to rapidly build tools that use these technologies to develop more robust and usable technologies

9.2.1 Background

Currently Computer Forensic technologies are being developed in an ad-hoc, as needed fashion. Since criminal investigators typically deal with computer and network data in a post-mortem sense, tools are developed and used after a crime, break-in, theft or disruption of service, to help the investigators discover the guilty. In the case of current intrusion detection and prevention tools, information pertaining to network activity is gathered. This information is typically derived from a single point of view or perspective. This perspective is generally close to the resources we are trying to protect

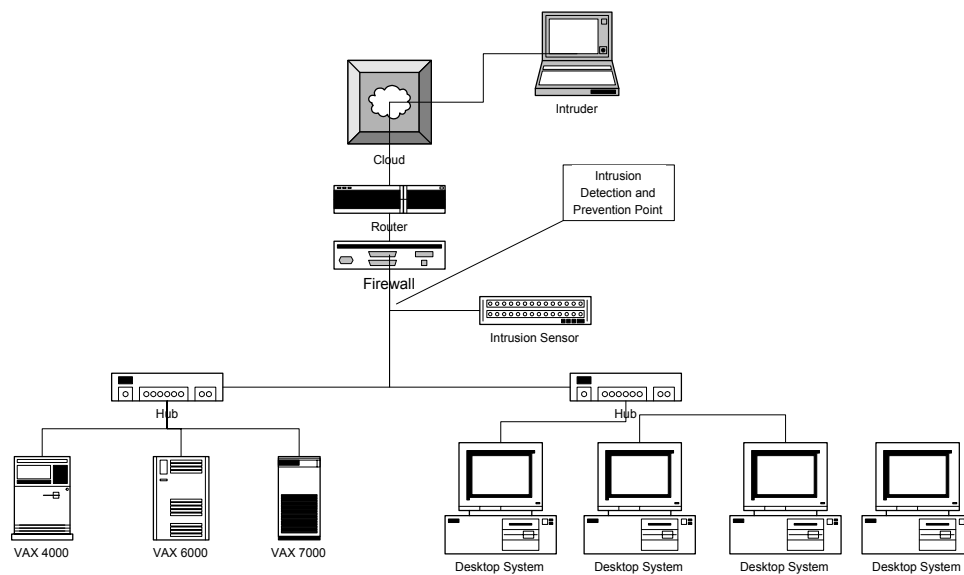


Figure 9.2 Typical Intrusion Detection System Deployment

In both military and criminal situations, the information that is essential for improving the detect, react and recover paradigm relates to the assailant's activities outside as well as inside our domain. Most of the current technologies that have been researched and developed address the "low hanging fruit". For example, a substantial amount of work has been done in imaging or preservation of evidence. This development or engineering was born out of the need to duplicate evidence in seized computers. Thus, the technology development has focused on developing tools that will preserve or image the media that we most commonly deal with. As the media that we recover becomes larger, we add "band aids" on to existing media imaging tools to assist in splitting image data pieces that will fit on existing optical or magnetic-optical devices. (both fraught with problems), instead of researching and developing the imaging techniques and media to be used in forensic investigations

The Roadmap must encourage research into enabling technologies that provide the forensic tool developers with technology that can be applied to a broad range of computer and network forensic tools. We think it may not be in the best interest of AFRL to focus R&D dollars on activities such as a general forensic toolkit due to the following factors:

- The use and application of the new core technologies may be very different for military, commercial and law-enforcement purposes, and these organizations will likely need to work together to prevent, detect and recover in the future in a coordinated fashion
- The actual technical break-thru's that are possible in developing a toolkit are limited, and will most likely be pursued and developed by commercial vendors or other government concerns
- To obtain technological superiority we must advance the research and development activities that will solve hard problems not the "low hanging fruit"
- We must define those areas of technology research and development that will significantly advance our technical superiority and allow commercial vendors and computer and network stake-holders (military, law-enforcement, banking and finance, utilities, etc) to integrate these solutions into their own tools and kits.













9.2.2 Interviews Conducted

The Computer Forensic Technology Roadmap is derived from WetStone Technologies, ECII and Dr. Gary Gordon's interviews with Computer Forensic Technology stake-holders that were contacted during the course of this study. Additional research was completed by reviewing journal articles, web resources, and news related information. In addition, WetStone Technologies supervised a group of Syracuse University Law Students to provide us with a report on Computer Forensics and Intrusion Detection and prevention technologies and market assessment.

9.2.3 Key Findings

The key findings of the Roadmap are broken down into the following four areas:

1. Identification of “gaps” in current computer forensic technologies that are hindering the investigative process. We classify these “gaps” into the following categories
 - a) Core Technology Advancement Needed
 - b) Adaptation of other Technologies Needed
 - c) Performance / Resource Limited
 - d) Legal or Privacy Limitations
2. Identification of future “threats” that cannot be currently countered, and where advanced research is necessary. In this area we will identify the threat and predict the consequences or cost of not addressing the threat
3. Identification of COTS technologies that will naturally evolve from the commercial or government sector to address the current “gaps” or future “threats”
4. Finally, we begin to define the core technology research and advancements that we feel are necessary. Based upon our current research findings, these areas will not be addressed by naturally evolving COTS or GOTS technologies. In addition to identifying the core technologies, we rank the importance based upon the risk or threats perceived (see figures 9.3, 9.4, and 9.5 below)

Computer Forensic Technology "GAPS"	Core Technologies	Technology Adaptation	Performance and Resource	Legal or Privacy
	Needed	Needed	Limited	Limited
Evidenciary Media				
Media Imaging Technology				
Steganography Detection and Recovery				
Encryption Detection and Recovery				
Network Based Evidence Mining Technologies				
Timelining of Computer Evidence				
Evidence Information Extraction and Reporting				
File Viewing Technologies				
Evidence Searching Technologies				
Evidence Correlation Technologies				



Mission Critical Gap



Serious Gap

Figure 9.3 Computer Forensics Technology Roadmap “The Gaps”.






























	6.1 Research Needed	6.2 Research Needed	6.3 & 6.4 R&D Needed
Future Threats			
Wide Use of Information Hiding Technologies			
Coordinated Wide Scale Computer Infrastructure Attacks			
Internet Coordinated Criminal and Terrorist Activity			
Insider Coordinated Theft and Distruction			
Intellectual Property Theft			



Figure 9.4 Computer Forensics Technology Roadmap “Future Threats”.

Core Technology Areas	Risk	Payoff	Timeframe Needed
Media Advancement Technologies			18-36 Months
Media Imaging Technologies			12-18 Months
Steganography Detection and Recovery			18-24 Months
Encryption Detection and Recovery			18-24 Months
Internet Forensics			9-24 Months
Evidence Correlation			6-18 Months
Evidence Mining			6-18 Months

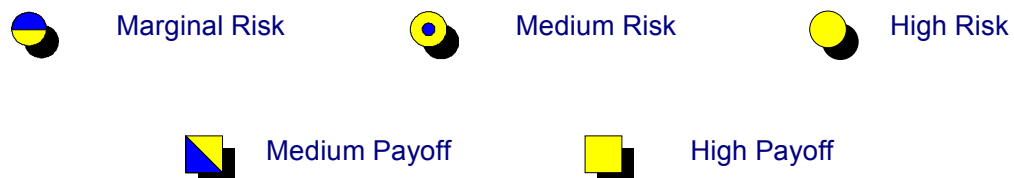


Figure 9.5 Computer Forensics Technology Roadmap “Core Technologies”

10 References

1. Adapted from Vagon International Limited, www.vogon.co.uk
2. Applied Cryptography Second Addition, John Wiley & Sons, Inc. 1996, by Bruce Schneier.
3. Ball v. State of New York, 101 Misc. 2d 554, 421 N.Y.S. 2d 328 (Ct.Cl. 1979).
4. Eugene H. Spafford, and Stephen A. Weeber, "Software Forensics: Can we Track Code to its Authors", Purdue Technical Report CSD-TR 92-010, February, 1992.
5. Forensic Information Warfare Requirements Study, Monthly Status Report, 9/2/98, AFRL Contract # F30602-C-98-0243.
6. Handbook of Applied Cryptography, CRC Press 1996. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
7. Hosmer, C.D. "Securing a Connected World", Eighth Annual Electronic Crime Investigative Institute (ECII) Conference, October 1997.
8. <http://home.earthlink.net/~jmellon/index.html#What>, Key Computer Service, Inc.
9. <http://knock-knock.com/forens01.htm>, Judd Robbins, Computer Forensics Specialist.
10. <http://police2.ucr.edu/evidence2.htm> Examination and Documentation of the Crime Scene by George Schiro forensic Scientist, Louisiana State Police Crime Laboratory
11. <http://r4149.resnet.cornell.edu/software/macslack/index.html#aboutSlack> Cornell University, Department of Computer Science.
12. <http://wings.buffalo.edu/Complaw/CompLawPapers/printup.html>, "Discovery of Computer Data", SUNY School of Law.
13. <http://www.cops.org/procedure.html>, IACIS.
14. <http://www.forensics-intl.com> New Technologies, Inc.
15. <http://www.foresic-computing.com/archives/diva.html> Data Integrity Verification and Authentication (DIVA), Jim Bates, Technical Director Computer Forensics Ltd.
16. <http://www.geek-girl.com/ids/0152.html> Tripwire 2.1 Release, Gene Kim gkim@cs.arizona.edu, Gene Spafford spaf@cs.purdue.edu, 30 August 1994
17. <http://www.geocities.com/CapitolHill/5244/time0002.html>
18. <http://www.jmacent.com>, JMac Enterprises
19. <http://www.secure-data.com/art7.html> Computer Evidence Processing The Third Step - Preserve the Electronic Crime Scene by Michael R. Anderson
20. International Association of Computer Investigative Specialists, <http://www.cops.org/procedure.html>,
21. Laurie Thomas Lee, Watch Your E-mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop", 28 J. Marshall L. Rev. 139 (1994).
22. Michael R. Anderson, "Electronic Fingerprints Computer Evidence Comes of Age", www.secure-data.com, April, 1998
23. New York State Police Forensic Investigation Center.
24. Richard G. Power, Computer Security Institute, "Testimony Before the Permanent Subcommittee on Investigations, U.S. Senate Committee on Governmental Affairs, June, 1996.
25. TAKE-DOWN The pursuit and capture of Kevin Mitnick, Americas Most Wanted Computer Outlaw, by Tsutomu Shimomura.
26. W. Diffie and M.E. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, v. 67, n. 3, Mar 1979, pp. 397-427.
27. www.vogon.co.uk Vagon International Limited.